UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/563,797	01/09/2006	Naoki Yamamoto	2005_1975A	5364

513   7590   02/09/2009
WENDEROTH, LIND & PONACK, L.L.P.
2033 K STREET N. W.
SUITE 800
WASHINGTON, DC 20006-1021

EXAMINER
POGMORE, TRAVIS D

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
02/09/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
Office Action Summary	10/563,797	YAMAMOTO ET AL.
	Examiner	Art Unit	
	Travis Pogmore	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _29 December 2008_.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _35-62_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _35-62_ is/are rejected.

7)☒ Claim(s) _59 and 60_ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1.   This action is in response to the request for reconsideration filed December 29, 2008.

2.   Claims 35-62 are currently pending. Claims 1-34 have been canceled. Claims 35-62 are new.

3.   Applicant's arguments, with regards to claims 35-62, filed December 29, 2008 have been fully considered but they are not persuasive.

Examiner Notes

4.   Examiner cites particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that, in preparing responses, the applicant fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

5.   The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Objections

6.   Applicant's arguments, see page 16, and respective cancellations with respect to the informalities of claims 1 and 6 have been fully considered and are persuasive. The objections thereof have been withdrawn.

7.   Claim 59 is objected to because of the following informalities: In lines 7-8 it recites "the information regarding the generations of the media keys." There is insufficient antecedent basis for this limitation in the claim as only "information regarding the generations of the plural device keys" was previously recited. For the purposes of examination it will be assumed that this should read "plural device keys" and not "media keys."

8.   Claim 60 is objected to because of the following informalities: In the seventh paragraph it recites "each of said plurality recording apparatuses belongs to either the first category or the second category." There is insufficient antecedent basis for this limitation in the claim as only categories for reproduction apparatuses was previously recited. For the purposes of examination it will be assumed that this should read "reproduction apparatuses" and not "recording apparatuses." Appropriate correction is required.

Claim Rejections – 35 USC § 101

9.   Claim 53 is rejected under 35 U.S.C. 101 as directed to non-statutory subject matter of software, *per se*. On page 24, line 31 to page 25, line 2 of the amended instant specification as filed, applicant has provided evidence that applicant intends

embodiments of the invention to include those implemented entirely in software. As

such, the claim(s) lack(s) the necessary physical articles or objects to constitute a

machine or manufacture within the meaning of 35 U.S.C. 101. It/they is/are clearly not a

series of steps or acts to be a process nor is/are it/they a combination of chemical

compounds to be a composition of matter. As such, it/they fail(s) to fall within a statutory

category. It/they is/are at best, functional descriptive material *per se*.

Descriptive material can be characterized as either "functional descriptive

material" or "nonfunctional descriptive material." Both types of "descriptive material" are

non-statutory when claimed as descriptive material *per se*, 33 F.3d at 1360, 31 USPQ2d

at 1759. When functional descriptive material is recorded on some computer-readable

medium, it becomes structurally and functionally interrelated to the medium and will be

statutory in most cases since use of technology permits the function of the descriptive

material to be realized. Compare *In re Lowry*, 32 F.3d 1579, 1583-84, 32 USPQ2d

1031, 1035 (Fed. Cir. 1994).

Merely claiming non-functional descriptive material, i.e. abstract ideas, stored on

a computer-readable medium, in a computer, or on an electromagnetic carrier signal,

does not make it statutory. See *Diehr*, 450 U.S. at 185-86, 209 USPQ at 8 (noting that

the claims for an algorithm in *Benson* were unpatentable as abstract ideas because

"[t]he sole practical application of the algorithm was in connection with the programming

of a general purpose computer.").

Claims 54-59 are rejected under 35 U.S.C. 101 as non-statutory for at least the

reason stated above. Claims 54-59 are dependent upon claim 53; however, they do not

add any feature or subject matter that would solve any of the non-statutory deficiencies

of claim 53.

Claim Rejections – 35 USC § 102

10.   Claim 62 is rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent

No. 6,118,873 (hereinafter "Lotspiech").

Lotspiech teaches a reproduction method for use in a reproduction apparatus

which belongs to one of plural categories and reproduces an encrypted content

recorded on a recording medium (column 2, lines 18-27 and column 5, lines 34-41,

where the M sets dimension are the plural categories),

wherein on the recording medium, at least the plurality of revocation data

generated based on a media key and a device key held by the reproduction apparatus

and intended for revoking the device key held by the reproduction apparatus (column

10, lines 35-41, it is inherent that in order to "broadcast" the "session key block" (i.e.

revocation data) and encrypted content in the form of a DVD movie as suggested it

must be on a recording medium, in particular a DVD), the encrypted content generated

by encrypting a content based on the media key (column 4, lines 45-52 and column 6,

lines 32-41, it is inherent that a session key (i.e. media key) used as a "common key" as

recited must be used for encryption as well as the explicitly stated decryption), and

information regarding generations of the plural device keys are record (Fig. 12, the

"Update Device Key Message," (i.e. information regarding the generation of the device

keys, as described further in column 9, lines 1-33)), and

said reproduction method comprises:

a read-out step of reading out, from the recording medium: the plurality of

revocation data corresponding to the reproduction apparatus; the information regarding

the generations of the plural device keys; and the encrypted content (column 2, lines

10-13); and

a decryption step of decrypting the encrypted content based on the plurality of

revocation data read out and the information regarding the generations of the plural

device keys (column 2, lines 13-17).

Claim Rejections – 35 USC § 103

11.   Claims 35-36, 40-42, 46-48, 52-54, and 58-61 are rejected under 35 U.S.C.

103(a) as being unpatentable over Lotspiech.

As to claim 35, Lotspiech teaches a copyright protection system comprising: a

recording apparatus configured to encrypt a content and to record the encrypted content

(Fig. 1, elements 12 and 14, 12 being the recording apparatus and 14 an encryption

module);

a recording medium on which the encrypted content is recorded (column 10,

lines 35-41, in particular it recites DVD movies); and

a plurality of reproduction apparatuses, each of which is configured to read out

and decrypt the encrypted content recorded on said recording medium (column 1, line

67 to column 2 line 2 and column 2, lines 10-17, the "plural user devices" being the

reproduction apparatuses),

wherein each of said plurality of reproduction apparatuses is one of either a first

plurality of reproduction apparatuses which belong to a first category and hold plural

device keys and information regarding generation of the plural device keys or a second

plurality of reproduction apparatuses (column 1, line 66 to column 2, line 2),

said recording apparatus is configured (a) to generate, for said plurality of

reproduction apparatuses and based on a media key and the device key held by each

of said plurality of reproduction apparatuses, a plurality of revocation data intended for

revoking a device key held by a specific reproduction apparatus of a respective

category (Abstract, lines 9-14 and column 2, lines 2-10, as recited the "session key

block" is created by using the encrypting session numbers (i.e. the media keys) with the

entire set of device keys and thus each of the categories and any "dummy number(s)"

along with the other valid session numbers are the revocation data), (b) to generate the

encrypted content which is the content encrypted based on the media key (column 4,

lines 45-52 and column 6, lines 32-41, it is inherent that a session key (i.e. media key)

used as a "common key" as recited must be used for encryption as well as the explicitly

stated decryption), and (c) to record the plurality of revocation data, the information

regarding the generation of the device keys for generating the plurality of revocation

data, and the encrypted content onto said recording medium (Fig. 6, elements 52 and

54, Fig. 12, as recited the "session key block," (i.e. revocation data), the "encrypted

program" (i.e. encrypted content), and the "Update Device Key Message," (i.e.

information regarding the generation of the device keys, as described further in column

9, lines 1-33)), and

the first plurality of reproduction apparatuses are each configured (a) to read out,

from said recording medium, the plurality of revocation data corresponding to said first

plurality of reproduction apparatuses, the information regarding the generations of the

plural device keys, and the encrypted content (column 2, lines 10-17 and column 9,

lines 1-33, as recited the session keys (including any "dummy numbers") are the

revocation data and the Update Device Key Message is the information regarding the

generations of the plural device keys), and (b) to decrypt the encrypted content based

on the plurality of revocation data read out and the information regarding the generation

of the plural device keys (column 2, lines 13-17),

the second plurality of reproduction apparatuses are each configured (a) to read

out, from said recording medium, the plurality of revocation data corresponding to said

second plurality of reproduction apparatuses and the encrypted content (column 2, lines

10-17, as recited the session keys (including any "dummy numbers") are the revocation

data), and (b) to decrypt the encrypted content based on the plurality of revocation data

read out (column 2, lines 13-17), but does not specifically teach wherein the second

plurality of reproduction devices belong to a second category and hold only one device

key.

However, wherein the second plurality of reproduction devices belong to a

second category and hold only one device key is well known and expected in the art

(e.g. European Patent Application Pub. No. EP 0969667 A2 (hereinafter "Masuda"),

page 2, paragraph 3, a single "Master key issued to each of the subscriber terminals").

Thereby official notice is taken.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Lotspiech to allow for devices possessing single device keys since this is well known and expected in the art and would enable interaction with new user devices possessing multiple device keys (as in Lotspiech) as well as legacy devices.

As to claim 36, Lotspiech teaches wherein each one of the plurality of revocation data is encrypted media key data which is the media key encrypted using a device key held by said plurality of reproduction apparatuses of a corresponding category,

the first plurality of reproduction apparatuses are each configured (a) to hold the plural device keys, (b) to read out, from said recording medium, the corresponding encrypted media key data, the information regarding the generation of the plural device keys, and the encrypted content (column 2, lines 10-17 and column 9, lines 1-33, the Update Device Key Message being the information regarding the generations of the plural device keys), (c) to select one among the plural device keys based on the information regarding the generation of the plural device keys, (d) to obtain the media key by decrypting the encrypted media key data using the selected device key (column 2, lines 30-38, the selected device key being "i" which matches the session (i.e. media) key to be decrypted), and (e) to decrypt the encrypted content based on the obtained media key (column 2, lines 13-17), and

the second plurality of reproduction apparatuses are each configured (a) to read out, from said recording medium, the corresponding encrypted media key data and the

encrypted content (column 2, lines 10-17), (b) to obtain the media key by decrypting the

encrypted media key data using the held device key (column 2, lines 30-38), and (c) to

decrypt the encrypted content based on the obtained media key (column 2, lines 13-17).

As to claim 40, Lotspiech teaches wherein each of the first plurality of

reproduction apparatuses includes:

a read-out apparatus of a second category configured to read out and perform a

part of a decryption process on the encrypted content recorded on said recording

medium (column 1, lines 30-38, e.g. a DVD player in combination with a set-top box);

and

a decryption apparatus of a first category, connected to said read-out apparatus

of the second category, configured to perform a part of the decryption process on the

encrypted content (column 1, lines 30-38, e.g. a digital television),

said recording apparatus is configured (a) to generate, based on a media key

and on a device key held by each of said decryption apparatus of the first category, a

plurality of first revocation data intended for revoking a device key held by a specific

decryption apparatus of the first category, (b) to generate, based on a media key and on

a device key held by each of apparatuses of the second category, a plurality of second

revocation data intended for revoking a device key held by a specific apparatus of the

second category (Abstract, lines 9-18 and column 2, lines 2-10, as recited the "session

key block" is created by using the encrypting session numbers (i.e. the media keys) with

the entire set of device keys and any "dummy number(s)" along with the other valid

session numbers are the revocation data), (c) to generate an encrypted content which is

the content encrypted based on the media key (column 4, lines 45-52 and column 6,

lines 32-41, it is inherent that a session key (i.e. media key) used as a "common key" as

recited must be used for encryption as well as the explicitly stated decryption), and (d)

to record at least the plurality of first revocation data, information regarding the

generation of the plural device keys for generating the plurality of first revocation data,

the plurality of second revocation data, and the encrypted content onto said recording

medium (Fig. 6, elements 52 and 54, Fig. 12, as recited the "session key block," (i.e.

revocation data), the "encrypted program" (i.e. encrypted content), and the "Update

Device Key Message," (i.e. information regarding the generation of the device keys, as

described further in column 9, lines 1-33)),

the second plurality of reproduction apparatuses are each configured to read out

the plurality of second revocation data and the encrypted content from said recording

medium (column 2, lines 10-13), and to decrypt the encrypted content based on the

plurality of second revocation data read out (column 2, lines 13-17), and

in each of the first plurality of reproduction apparatuses:

said read-out apparatus of the second category is configured (a) to read out,

from said recording medium, the plurality of first revocation data, the information

regarding the generations of the plural device keys, the plurality of second revocation

data, and the encrypted content (column 2, lines 10-13), and (to) supply intermediate

data, the information regarding the generations of the plural device keys, and the

plurality of first revocation data to said decryption apparatus of the first category, the

intermediate data being the encrypted content on which a part of the decryption process

has been performed based on the plurality of second revocation data (column 2, lines

13-17 and column 9, lines 38-49, the set-top box receives the broadcast from the DVD

player, any session-key block (which includes the second revocation data) is passed

through the set-top box and the content is re-encrypted to allow only legitimate devices

to view or record it); and

said decryption apparatus of the first category is configured to obtain the content

by performing the decryption process on the intermediate data, based on the plurality of

first revocation data and the information regarding the generations of the plural device

keys supplied by said read-out apparatus of the second category (column 9, lines 44-

46).

As to claim 41, Lotspiech teaches a recording apparatus which encrypts a

content and records the encrypted content (Fig. 1, elements 12 and 14, 12 being the

recording apparatus and 14 an encryption module), the content being reproduced by

first reproduction apparatuses which belong to a first category and hold plural device

keys and information regarding generations of the plural device keys and by second

reproduction apparatuses (column 1, line 66 to column 2, line 2 and column 9, lines 1-

33, the Update Device Key Message is the information regarding generations of the

plural device keys),

wherein said recording apparatus (a) generates, for a plurality of reproduction

apparatuses and based on a media key and the device key held by each of the plurality

of reproduction apparatuses, a plurality of revocation data intended for revoking a

device key held by a specific reproduction apparatus belonging to respective categories

(Abstract, lines 9-14 and column 2, lines 2-10, as recited the "session key block" is

created by using the encrypting session numbers (i.e. the media keys) with the entire

set of device keys and thus each of the categories and any "dummy number(s)" along

with the other valid session numbers are the revocation data), (b) generates an

encrypted content which is the content encrypted based on the media key (column 4,

lines 45-52 and column 6, lines 32-41, it is inherent that a session key (i.e. media key)

used as a "common key" as recited must be used for encryption as well as the explicitly

stated decryption), and (c) records the plurality of revocation data, the information

regarding the generations of the plural device keys for generating the plurality of

revocation data, and the encrypted content onto a recording medium (Fig. 6, elements

52 and 54, Fig. 12, as recited the "session key block," (i.e. revocation data), the

"encrypted program" (i.e. encrypted content), and the "Update Device Key Message,"

(i.e. information regarding the generation of the device keys, as described further in

column 9, lines 1-33)), but does not specifically teach wherein the second reproduction

apparatuses belong to a second category and hold only one device key.

However, wherein the second reproduction apparatuses belong to a second

category and hold only one device key is well known and expected in the art (e.g.

Masuda, page 2, paragraph 3, a single "Master key issued to each of the subscriber

terminals"). Thereby official notice is taken.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Lotspiech to allow for devices possessing single device keys since this is well known and expected in the art and would enable interaction with new user devices possessing multiple device keys (as in Lotspiech) as well as legacy devices.

As to claim 42, Lotspiech teaches wherein each one of the plurality of revocation data is encrypted media key data which is the media key encrypted using the device key held by the plurality of reproduction apparatuses of a corresponding category (column 2, lines 2-10, as recited the "session key block" is created by using the encrypting session numbers (i.e. the media keys) with the entire set of device keys and thus each category).

As to claim 46, Lotspiech teaches wherein said recording apparatus (a) generates, based on a media key and on a device key held by each of decryption apparatuses of the first category, a plurality of first revocation data intended for revoking a device key held by a specific decryption apparatus of the first category, (b) generates, based on a media key and on a device key held by apparatuses of the second category, a plurality second revocation data intended for revoking a device key held by a specific apparatus of the second category (Abstract, lines 9-18 and column 2, lines 2-10, as recited the "session key block" is created by using the encrypting session numbers (i.e. the media keys) with the entire set of device keys and any "dummy number(s)" along

with the other valid session numbers are the revocation data), and (c) generates an

encrypted content which is the content encrypted based on the media key (column 4,

lines 45-52 and column 6, lines 32-41, it is inherent that a session key (i.e. media key)

used as a "common key" as recited must be used for encryption as well as the explicitly

stated decryption), and (d) records at least plurality of first revocation data, information

regarding the generations of the plural device keys for generating the plurality of first

revocation data, a plurality of the second revocation data, and the encrypted content

onto the recording medium (Fig. 6, elements 52 and 54, Fig. 12, as recited the "session

key block," (i.e. revocation data), the "encrypted program" (i.e. encrypted content), and

the "Update Device Key Message," (i.e. information regarding the generation of the

device keys, as described further in column 9, lines 1-33)).

        As to claim 47, Lotspiech teaches a recording medium on which a content

reproduced by the plurality of reproduction apparatuses is recorded (column 10, lines

35-41, in particular it recites DVD movies), the plurality of reproduction apparatuses

including first reproduction apparatuses belonging to a first category and holding plural

device keys and information regarding generations of the plural device keys, and

second reproduction apparatuses (column 1, line 66 to column 2, line 2 and column 9,

lines 1-33, the Update Device Key Message is the information regarding generations of

the plural device keys),

        wherein on said recording medium, at least (i) a plurality of revocation data

generated based on a media key and the device key held by each of the plurality of

reproduction apparatuses and intended for revoking the device key held by the specific

reproduction apparatus of the respective categories (column 10, lines 35-41, it is

inherent that in order to "broadcast" the "session key block" (i.e. revocation data) and

encrypted content in the form of a DVD movie as suggested it must be on a recording

medium, in particular a DVD), (ii) information regarding generations of the plural device

keys for generating the plurality of revocation data (Fig. 12, the "Update Device Key

Message," (i.e. information regarding the generation of the device keys, as described

further in column 9, lines 1-33)), and (iii) an encrypted content generated by encrypting

the content based on the media key are recorded (column 4, lines 45-52 and column 6,

lines 32-41, it is inherent that a session key (i.e. media key) used as a "common key" as

recited must be used for encryption as well as the explicitly stated decryption), but does

not specifically teach wherein the second reproduction apparatuses belong to a second

category and hold only one device key.

However, wherein the second reproduction apparatuses belong to a second

category and hold only one device key is well known and expected in the art (e.g.

Masuda, page 2, paragraph 3, a single "Master key issued to each of the subscriber

terminals"). Thereby official notice is taken.

Therefore, it would have been obvious to a person having ordinary skill in the art

at the time the invention was made to modify Lotspiech to allow for devices possessing

single device keys since this is well known and expected in the art and would enable

interaction with new user devices possessing multiple device keys (as in Lotspiech) as

well as legacy devices.

As to claim 48, Lotspiech teaches wherein each one of the plurality of revocation

data is encrypted media key data which is the media key encrypted using the device

key held by the plurality of reproduction apparatuses of a corresponding category

(column 2, lines 2-10, as recited the "session key block" is created by using the

encrypting session numbers (i.e. the media keys) with the entire set of device keys and

thus each category).

As to claim 52, Lotspiech teaches wherein on said recording medium, at least (i)

a plurality of first revocation data generated based on the media key and on plural

device keys held by decryption apparatuses of the first category and intended for

revoking a device key held by a specific decryption apparatus of the first category

(Abstract, lines 9-18 and column 2, lines 2-10, as recited the "session key block" is

created by using the encrypting session numbers (i.e. the media keys) with the entire

set of device keys and any "dummy number(s)" along with the other valid session

numbers are the revocation data), (ii) information regarding generations of the plural

device keys for generating the plurality of first revocation data (column 9, lines 1-33, the

Update Device Key Message is the information regarding the generations of the plural

device keys), (iii) a plurality of second revocation data generated based on a media key

and on plural device keys held by apparatuses of the second category and intended for

revoking a device key held by a specific apparatus of the second category (Abstract,

lines 9-18 and column 2, lines 2-10, as recited the "session key block" is created by

using the encrypting session numbers (i.e. the media keys) with the entire set of device keys and any "dummy number(s)" along with the other valid session numbers are the revocation data), and (iv) the encrypted content which is the content on which an encryption process has been performed based on the media key are recorded (column 4, lines 45-52 and column 6, lines 32-41, it is inherent that a session key (i.e. media key) used as a "common key" as recited must be used for encryption as well as the explicitly stated decryption).

As to claim 53, Lotspiech teaches a reproduction apparatus and reproduces an encrypted content recorded on a recording medium,

wherein on the recording medium, at least revocation data generated based on a media key and a device key held by said reproduction apparatus and intended for revoking the device key held by said reproduction apparatus, an encrypted content generated by encrypting a content based on the media key, and information regarding generations of the plural device keys for generating the revocation data (Fig. 6, elements 52 and 54, Fig. 12, as recited the "session key block," (i.e. revocation data), the "encrypted program" (i.e. encrypted content), and the "Update Device Key Message," (i.e. information regarding the generation of the device keys, as described further in column 9, lines 1-33)), and

said reproduction apparatus (a) reads out, from the recording medium, the revocation data, corresponding to said reproduction apparatus, the information regarding the generations of the plural device keys, and the encrypted content (column

2, lines 10-17 and column 9, lines 1-33, as recited the session keys (including any "dummy numbers") are the revocation data and the Update Device Key Message is the information regarding the generations of the plural device keys), and (b) decrypts the encrypted content based on the plurality of revocation data read out and the information regarding the generations of the plural device keys (column 2, lines 13-17), but does not specifically teach wherein the reproduction apparatus belongs to one of plural categories.

However, Lotspiech teaches reproduction apparatuses with plural device keys (i.e. a first category) and reproduction devices with only one device key (i.e. a second category) are well known and expected in the art (e.g. Masuda, page 2, paragraph 3, a single "Master key issued to each of the subscriber terminals"). Thereby official notice is taken.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Lotspiech to allow for devices possessing single device keys since this is well known and expected in the art and would enable interaction with new user devices possessing multiple device keys (as in Lotspiech) as well as legacy devices.

As to claim 54, Lotspiech teaches wherein the revocation data is encrypted media key data which is the media key encrypted using the device key data held by said reproduction apparatus (column 2, lines 2-10, as recited the "session key block" is

created by using the encrypting session numbers (i.e. the media keys) with the entire

set of device keys), and

said reproduction apparatus (a) holds plural device keys, (b) reads out, from the

recording medium, the encrypted media key data, the information regarding the

generations of the plural device keys, and the encrypted content (column 2, lines 10-17

and column 9, lines 1-33, the Update Device Key Message being the information

regarding the generations of the plural device keys), (c) selects one among the plural

device keys based on the information regarding the generations of the plural device

keys, (d) obtains the media key by decrypting the encrypted media key data using the

selected device key (column 2, lines 30-38, the selected device key being "i" which

matches the session (i.e. media) key to be decrypted), and (e) decrypts the encrypted

content based on the obtained media key (column 2, lines 13-17).

As to claim 58, Lotspiech teaches wherein on the recording medium, at least (i) a

plurality of first revocation data generated based on the media key and on a device key

held by each of decryption apparatuses of a first category and intended for revoking a

device key held by a specific decryption apparatus of the first category (Abstract, lines

9-18 and column 2, lines 2-10, as recited the "session key block" is created by using the

encrypting session numbers (i.e. the media keys) with the entire set of device keys and

any "dummy number(s)" along with the other valid session numbers are the revocation

data), (ii) information regarding generations of the plural device keys for generating the

plurality of first revocation data (column 9, lines 1-33, the Update Device Key Message

is the information regarding the generations of the plural device keys), (iii) a plurality of

second revocation data generated based on a media key and on a device key held by

each of apparatuses of a second category and intended for revoking a device key held

by a specific apparatus of the second category (Abstract, lines 9-18 and column 2, lines

2-10, as recited the "session key block" is created by using the encrypting session

numbers (i.e. the media keys) with the entire set of device keys and any "dummy

number(s)" along with the other valid session numbers are the revocation data), and (iv)

the encrypted content which is the content on which an encryption process has been

performed based on the media key are recorded (column 4, lines 45-52 and column 6,

lines 32-41, it is inherent that a session key (i.e. media key) used as a "common key" as

recited must be used for encryption as well as the explicitly stated decryption), and said

reproduction apparatus belongs to the second category and reads out, from the

recording medium, the plurality of second revocation data and the encrypted content,

and decrypts the encrypted content based on the plurality of second revocation data

(column 2, lines 10-17).

As to claim 59, Lotspiech teaches comprising:

a read-out apparatus belonging to the second category and configured to read

out, from the recording medium, the plurality of first revocation data, the plurality of

second revocation data, the information regarding the generations of the plural device

keys, and the encrypted content (column 2, lines 10-13), to generate intermediate data

which is the encrypted content on which a part of a decryption process has been

performed based on the plurality of second revocation data, and to output the generated

intermediate data, the information regarding the generations of the media keys, and the

first revocation (column 2, lines 13-17 and column 9, lines 38-49, the set-top box

receives the broadcast from the DVD player, any session-key block (which includes the

second revocation data) is passed through the set-top box and the content is re-

encrypted to allow only legitimate devices to view or record it); and

a decryption apparatus belonging to the first category and configured to obtain

the content by performing a decryption process on the intermediate data, based on the

plurality of first revocation data and the information regarding the generations of the

plural device keys (column 9, lines 44-46).

As to claim 60, Lotspiech teaches a copyright protection system comprising:

a key generation apparatus configured to generate and record a plurality of

revocation data necessary for encrypting and decrypting a content (Fig. 1, elements 12

and 14, 12 being the recording apparatus and 14 an encryption module),

a plurality recording apparatuses, each of which is configured to encrypt a

content and to record the encrypted content (Fig. 6, elements 52 and 54, as recited the

"session key block" and the "encrypted program");

a recording medium on which the encrypted content and the plurality of

revocation data are recorded (column 10, lines 35-41, in particular it recites DVD

movies); and

a plurality of reproduction apparatuses, each of which is configured to read out

and decrypt the encrypted content recorded on said recording medium (column 1, line

67 to column 2 line 2 and column 2, lines 10-17, the "plural user devices" being the

reproduction apparatuses),

wherein each of said plurality of reproduction apparatuses is one of either first

reproduction apparatuses which belong to a first category and hold plural device keys

and information regarding generations of the plural device keys or second reproduction

apparatuses (column 1, line 66 to column 2, line 2 and column 9, lines 1-33),

said key generation apparatus is configured (a) to generate, for said plurality of

reproduction apparatuses and based on a media key and the device key held by each

of said plurality recording apparatuses or plurality of reproduction apparatuses, the

plurality of revocation data intended for revoking a device key held by a specific

recording apparatus or a specific reproduction apparatus of the respective categories

(tract, lines 9-18 and column 2, lines 2-10, as recited the "session key block" is created

by using the encrypting session numbers (i.e. the media keys), and (b) to record the

generated a plurality of revocation data and the information regarding the generations of

the plural device keys for generating the plurality of revocation data onto said recording

medium (Fig. 6, element 52 and Fig. 12, as recited the "session key block," (i.e.

revocation data) and the "Update Device Key Message," (i.e. information regarding the

generation of the device keys, as described further in column 9, lines 1-33)),

said plurality recording apparatuses are each configured (a) to read out, from

said recording medium, the plurality of revocation data for the category to which said

recording apparatus belongs (column 9, lines 38-44), (b) to generate the encrypted content by encrypting the content based on the plurality of revocation data read out (column 9, lines 44-46), and (c) to record the generated encrypted content on said recording medium (column 9, lines 36-40 and 44-46, it is inherent that a device such as a VCR which generates encrypted data and then allows other devices to decrypt it must be able to record said encrypted data at some point),

the first plurality of reproduction apparatuses are each configured (a) to read out, from said recording medium, the plurality of revocation data corresponding to said first plurality of reproduction apparatuses, the information regarding the generations of the plural device keys, and the encrypted content (column 2, lines 10-17 and column 9, lines 1-33, as recited the session keys (including any "dummy numbers") are the revocation data and the Update Device Key Message is the information regarding the generations of the plural device keys), and (b) to decrypt the encrypted content based on the plurality of revocation data read out and the information regarding the generation of the plural device keys (column 2, lines 13-17),

the second plurality of reproduction apparatuses are each configured (a) to read out, from said recording medium, the plurality of revocation data corresponding to said second plurality of reproduction apparatuses and the encrypted content (column 2, lines 10-17, as recited the session keys (including any "dummy numbers") are the revocation data), and (b) to decrypt the encrypted content based on the plurality of revocation data read out (column 2, lines 13-17), but does not specifically teach wherein the second

reproduction apparatuses belong to a second category and hold only one device key,

nor

each of said plurality recording apparatuses belongs to either the first category or

the second category.

However, wherein the second plurality of reproduction devices belong to a

second category and hold only one device key is well known and expected in the art

(e.g. Masuda, page 2, paragraph 3, a single "Master key issued to each of the

subscriber terminals"), and

each of said plurality recording apparatuses belongs to either the first category or

the second category is also well known and expected in the art (it is inherent that an

apparatus possessing a device key must possess either one (i.e. belong to the second

category) or more (i.e. belong to the first category)). Thereby official notice is taken.

Therefore, it would have been obvious to a person having ordinary skill in the art

at the time the invention was made to modify Lotspiech to allow for devices possessing

single device keys since this is well known and expected in the art and would enable

interaction with new user devices possessing multiple device keys (as in Lotspiech) as

well as legacy devices.

As to claim 61, Lotspiech teaches a recording method for use in a recording

apparatus which encrypts a content reproduced by plurality of reproduction apparatuses

and records the encrypted content, the plurality of reproduction apparatuses including

first reproduction apparatuses belonging to a first category and holding plural device

keys and information regarding generations of the plural device keys, and second

reproduction apparatuses (column 1, line 66 to column 2, line 2), said method

comprising:

a step of generating, for the plurality of reproduction apparatuses and based on a

media key and the device key held by each of said plurality of reproduction

apparatuses, a plurality of revocation data intended for revoking a device key held by a

specific reproduction apparatus of the respective categories (Abstract, lines 9-18 and

column 2, lines 2-10, as recited the "session key block" is created by using the

encrypting session numbers (i.e. the media keys) with the entire set of device keys and

any "dummy number(s)" along with the other valid session numbers are the revocation

data);

an encrypted content generation step of generating the encrypted content by

encrypting the content, based on the media key (column 4, lines 45-52 and column 6,

lines 32-41, it is inherent that a session key (i.e. media key) used as a "common key" as

recited must be used for encryption as well as the explicitly stated decryption); and

a recording step of recording the plurality of revocation data, the information

regarding the generations of the plural device keys for generating the plurality of

revocation data, and the encrypted content onto the recording medium (Fig. 6, elements

52 and 54, Fig. 12, as recited the "session key block," (i.e. revocation data), the

"encrypted program" (i.e. encrypted content), and the "Update Device Key Message,"

(i.e. information regarding the generation of the device keys, as described further in

column 9, lines 1-33)), but does not specifically teach wherein the second reproduction apparatuses belong to a second category and hold only one device key.

However, wherein the second reproduction apparatuses belong to a second category and hold only one device key is well known and expected in the art (e.g. Masuda, page 2, paragraph 3, a single "Master key issued to each of the subscriber terminals"). Thereby official notice is taken.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Lotspiech to allow for devices possessing single device keys since this is well known and expected in the art and would enable interaction with new user devices possessing multiple device keys (as in Lotspiech) as well as legacy devices.

12.   Claims 37, 43, 49, and 55 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lotspiech in view of U.S. Patent Application Pub. No. US 2001/044897 A1 (hereinafter "Ishiguro").

As to claim 37, Lotspiech teaches the copyright protection system according to Claim 36, but does not specifically teach wherein said recording apparatus is configured to generate an encryption key based on the media key, and to encrypt the content based on the encryption key, and said plurality of reproduction apparatuses of the respective categories are each configured to generate a decryption key based on the

obtained media key, and to decrypt the encrypted content based on the generated

decryption key.

However, Ishiguro teaches wherein said recording apparatus is configured to

generate an encryption key based on the media key, and to encrypt the content based

on the encryption key (page 5, paragraph 73, lines 5-8 and 11-14), and said plurality of

reproduction apparatuses of the respective categories are each configured to generate

a decryption key based on the obtained media key, and to decrypt the encrypted

content based on the generated decryption key (page 5, paragraph 73, lines 8-11 and

14-16).

Therefore, it would have been obvious to a person having ordinary skill in the art

at the time the invention was made to modify Lotspiech to encrypt the content using an

additional key as in Ishiguro because it provides an additional layer of security.

As to claim 43, Lotspiech teaches the recording apparatus according to Claim 42,

but does not specifically teach wherein said recording apparatus generates an

encryption key based on the media key, and encrypts the content based on the

encryption key.

However, Ishiguro teaches wherein said recording apparatus generates an

encryption key based on the media key, and encrypts the content based on the

encryption key (page 5, paragraph 73, lines 11-14).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Lotspiech to encrypt the content using an additional key as in Ishiguro because it provides an additional layer of security.

As to claim 49, Lotspiech teaches the recording medium according to Claim 48, but does not specifically teach wherein the encrypted content is generated by encrypting the content, based on an encryption key generated based on the media key.

However, Ishiguro teaches wherein the encrypted content is generated by encrypting the content, based on an encryption key generated based on the media key (page 5, paragraph 73, lines 11-14).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Lotspiech to encrypt the content using an additional key as in Ishiguro because it provides an additional layer of security.

As to claim 55, Lotspiech teaches the reproduction apparatus according to Claim 54, but does not specifically teach wherein the encrypted content is generated by encrypting the content, based on an encryption key generated based on the media key, and said reproduction apparatus generates a decryption key based on the obtained media key, and decrypts the encrypted content based on the generated decryption key.

However, Ishiguro teaches wherein the encrypted content is generated by encrypting the content, based on an encryption key generated based on the media key ((page 5, paragraph 73, lines 5-8 and 11-14)), and said reproduction apparatus

generates a decryption key based on the obtained media key, and decrypts the

encrypted content based on the generated decryption key (page 5, paragraph 73, lines

8-11 and 14-16).

Therefore, it would have been obvious to a person having ordinary skill in the art

at the time the invention was made to modify Lotspiech to encrypt the content using an

additional key as in Ishiguro because it provides an additional layer of security.

13.   Claims 38-39, 44-45, 50-51, and 56-57 are rejected under 35 U.S.C. 103(a) as

being unpatentable over Lotspiech et al. in view of Masuda.

As to claim 38, Lotspiech teaches the copyright protection system according to

Claim 36, but does not specifically teach wherein said recording apparatus is configured

to encrypt the content using a content key, to generate encrypted content key data by

encrypting the content key using the media key, and to record the generated encrypted

content key data onto said recording medium, and said plurality of reproduction

apparatuses of the respective categories are each configured to read out the encrypted

content key data from said recording medium, to obtain the content key by decrypting

the encrypted content key data using the media key, and to decrypt the encrypted

content using the obtained content key.

However Masuda teaches wherein said recording apparatus is configured to

encrypt the content using a content key (page 2, lines 49-50, the "scramble key"), to

generate encrypted content key data by encrypting the content key using the media key

(page 2, lines 53-56 and page 3, line 11, where the "second key" is the media key), and

to record the generated encrypted content key data onto said recording medium (page

2, lines 56-58), and said plurality of reproduction apparatuses of the respective

categories are each configured to read out the encrypted content key from said

recording medium (page 2, line 58 to page 3, line 2), to obtain the content key by

decrypting the encrypted content key using the media key (page 3, lines 3-5), and to

decrypt the encrypted content using the obtained content key (page 3, lines 5-6).

Therefore, it would have been obvious to a person having ordinary skill in the art

at the time the invention was made to modify Lotspiech to encrypt the content using an

additional key as in Masuda because it provides an additional layer of security.

As to claim 39, Lotspiech teaches wherein each one of the plurality of revocation

data is encrypted media key data which is a media key for a corresponding category,

encrypted using the device key data held by said plurality of reproduction apparatuses

of a corresponding category (column 2, lines 2-10, as recited the "session key block" is

created by using the encrypting session numbers (i.e. the media keys) with the entire

set of device keys), and wherein also recorded onto the recording medium is the

information regarding the generations of the plural device keys for encrypting the media

key (Fig. 12, the "Update Device Key Message," (i.e. information regarding the

generation of the device keys, as described further in column 9, lines 1-33)), but does

not specifically teach said recording apparatus is configured to encrypt the content

using a content key, to generate a plurality of encrypted content key data by encrypting

the content key using the media keys corresponding to the category of said plurality of

reproduction apparatuses, and to record, onto said recording medium, at least

encrypted media key data, the plurality of encrypted content key data, and the

encrypted content,

the first plurality of reproduction apparatuses are each configured (a) to hold the

plural device keys, (b) to read out, from said recording medium, the information

regarding the generation of the plural device keys, the encrypted media key data for the

corresponding category, the encrypted content key data for the corresponding category,

and the encrypted content, (c) to select one among the plural device keys based on the

information regarding the generation of the plural device keys, (d) to obtain a media key

for the corresponding category by decrypting the encrypted media key data using the

selected device key, (e) to obtain the content key by decrypting the encrypted content

key data for the corresponding category using the obtained media key for the

corresponding category, and (f) to decrypt the encrypted content using the obtained

content key, nor

the second plurality of reproduction apparatuses are each configured (a) to read

out, from said recording medium, the encrypted media key data for the corresponding

category, the encrypted content key data for the corresponding category, and the

encrypted content, (b) to obtain the media key for the corresponding category by

decrypting the encrypted media key data using the held device key, (c) to obtain the

content key by decrypting the encrypted content key data for the corresponding

category using the obtained media key for the corresponding category, and (d) to

decrypt the encrypted content using the obtained content key.

However, Masuda teaches said recording apparatus is configured to encrypt the

content using a content key (page 2, lines 49-50, the "scramble key"), to generate a

plurality of encrypted content key data by encrypting the content key using the media

keys corresponding to the category of said plurality of reproduction apparatuses (page

2, lines 53-56 and page 3, line 11, where the "second key" is the session key block (i.e.

media key) as recited in Lotspiech), and to record, onto said recording medium, at least

encrypted media key data, the plurality of encrypted content key data, and the

encrypted content (Lotspiech, Fig. 6, elements 52 and 54, as recited the "session key

block" and the "encrypted program" and Masuda, page 2, lines 56-58),

the first plurality of reproduction apparatuses are each configured (a) to hold the

plural device keys (Lotspiech, column 1, line 67 to column 2, line 2), (b) to read out,

from said recording medium, the information regarding the generation of the plural

device keys, the encrypted media key data for the corresponding category, the

encrypted content key data for the corresponding category, and the encrypted content

(page 2, line 58 to page 3, line 2), (c) to select one among the plural device keys based

on the information regarding the generation of the plural device keys (Lotspiech, column

9, lines 14-17), (d) to obtain a media key for the corresponding category by decrypting

the encrypted media key data using the selected device key (Lotspiech, column 2, lines

30-38), (e) to obtain the content key by decrypting the encrypted content key data for

the corresponding category using the obtained media key for the corresponding

category (page 3, lines 3-5), and (f) to decrypt the encrypted content using the obtained

content key (page 3, lines 5-6), and

the second plurality of reproduction apparatuses are each configured (a) to read

out, from said recording medium, the encrypted media key data for the corresponding

category, the encrypted content key data for the corresponding category, and the

encrypted content (page 2, line 58 to page 3, line 2), (b) to obtain the media key for the

corresponding category by decrypting the encrypted media key data using the held

device key (Lotspiech, column 2, lines 30-38), (c) to obtain the content key by

decrypting the encrypted content key data for the corresponding category using the

obtained media key for the corresponding category (page 3, lines 3-5), and (d) to

decrypt the encrypted content using the obtained content key (page 3, lines 5-6).

Therefore, it would have been obvious to a person having ordinary skill in the art

at the time the invention was made to modify Lotspiech to encrypt the content using an

additional key as in Masuda because it provides an additional layer of security.

As to claim 44, Lotspiech teaches the recording apparatus according to Claim 42,

but does not specifically teach wherein said recording apparatus encrypts the content

using a content key, generates encrypted content key data which is the content key

encrypted using the media key, and records the generated encrypted key onto the

recording medium.

However, Masuda teaches wherein said recording apparatus encrypts the

content using a content key (page 2, lines 49-50, the "scramble key"), generates

encrypted content key data which is the content key encrypted using the media key

(page 2, lines 53-56 and page 3, line 11, where the "second key" is the media key), and

records the generated encrypted key onto the recording medium (page 2, lines 56-58).

Therefore, it would have been obvious to a person having ordinary skill in the art

at the time the invention was made to modify Lotspiech to encrypt the content using an

additional key as in Masuda because it provides an additional layer of security.

As to claim 45, Lotspiech teaches wherein each one of the plurality of revocation

data is encrypted media key data which is a media key for a corresponding category,

encrypted using the device key held by the plurality of reproduction apparatuses of the

corresponding category (column 2, lines 2-10, as recited the "session key block" is

created by using the encrypting session numbers (i.e. the media keys) with the entire

set of device keys), but does not specifically teach wherein said recording apparatus is

configured (a) to encrypt the content using a content key, (b) to generate a plurality of

encrypted content key data by encrypting the content key using the media keys

corresponding to the category of the reproduction apparatus, and (c) to record, onto the

recording medium, at least the encrypted media key data, the information regarding the

generations of the plural device keys for encrypting the media key, and the encrypted

content.

However, Masuda teaches wherein said recording apparatus is configured (a) to

encrypt the content using a content key (page 2, lines 49-50, the "scramble key"), (b) to

generate a plurality of encrypted content key data by encrypting the content key using

the media keys corresponding to the category of the reproduction apparatus (page 2,

lines 53-56 and page 3, line 11, where the "second key" is the session key block (i.e.

media key) as recited in Lotspiech), and (c) to record, onto the recording medium, at

least the encrypted media key data, the information regarding the generations of the

plural device keys for encrypting the media key, and the encrypted content (Lotspiech

Fig. 6, element 54, Fig. 12, as recited the "encrypted program" (i.e. encrypted content),

and the "Update Device Key Message," (i.e. information regarding the generation of the

device keys, as described further in column 9, lines 1-33) and Masuda, page 2, lines 56-

58).

Therefore, it would have been obvious to a person having ordinary skill in the art

at the time the invention was made to modify Lotspiech to encrypt the content using an

additional key as in Masuda because it provides an additional layer of security.

As to claim 50, Lotspiech teaches the recording medium according to Claim 48,

but does not specifically teach wherein the encrypted content is generated by

encrypting the content using a content key, and on said recording medium, encrypted

content key data is recorded, the encrypted content key data being generated by

encrypting the content key using the media key.

However, Masuda teaches wherein the encrypted content is generated by

encrypting the content using a content key (page 2, lines 49-50, the "scramble key"),

and on said recording medium, encrypted content key data is recorded (page 2, lines

56-58), the encrypted content key data being generated by encrypting the content key

using the media key (page 2, lines 53-56 and page 3, line 11, where the "second key" is

the media key).

Therefore, it would have been obvious to a person having ordinary skill in the art

at the time the invention was made to modify Lotspiech to encrypt the content using an

additional key as in Masuda because it provides an additional layer of security.

As to claim 51, Lotspiech teaches wherein each one of the plurality of revocation

data is encrypted media key data which is a media key for a corresponding category,

encrypted using the device key held by the plurality of reproduction apparatuses of the

corresponding category (column 2, lines 2-10, as recited the "session key block" is

created by using the encrypting session numbers (i.e. the media keys) with the entire

set of device keys), but does not specifically teach the encrypted content is generated

by encrypting the content using a content key, nor

on said recording medium, a plurality of encrypted content key data generated by

encrypting the content key using the media keys corresponding to the category of the

plurality of reproduction apparatuses are recorded.

However, Masuda teaches the encrypted content is generated by encrypting the

content using a content key (page 2, lines 49-50, the "scramble key"), and

on said recording medium, a plurality of encrypted content key data generated by

encrypting the content key using the media keys corresponding to the category of the

plurality of reproduction apparatuses are recorded (page 2, lines 56-58).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Lotspiech to encrypt the content using an additional key as in Masuda because it provides an additional layer of security.

As to claim 56, Lotspiech teaches the reproduction apparatus according to Claim 54, but does not specifically teach wherein the encrypted content is generated by encrypting the content using a content key, on the recording medium, encrypted content key data generated by encrypting the content key using the media key is recorded, and said reproduction apparatus (a) reads out the encrypted content key data from the recording medium, (b) obtains the content key by decrypting the encrypted content key data using the media key, and (c) decrypts the encrypted content using the obtained content key.

However, Masuda teaches wherein the encrypted content is generated by encrypting the content using a content key (page 2, lines 49-50, the "scramble key"), on the recording medium, encrypted content key data generated by encrypting the content key using the media key is recorded (page 2, lines 53-58 and page 3, line 11, where the "second key" is the media key), and said reproduction apparatus (a) reads out the encrypted content key data from the recording medium (page 2, line 58 to page 3, line 2), (b) obtains the content key by decrypting the encrypted content key data using the media key (page 3, lines 3-5), and (c) decrypts the encrypted content using the obtained content key (page 3, lines 5-6).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Lotspiech to encrypt the content using an additional key as in Masuda because it provides an additional layer of security.

As to claim 57, Lotspiech teaches wherein the revocation data is encrypted media key data which is a media key for a corresponding category, encrypted using the device key held by said reproduction apparatus (column 2, lines 2-10, as recited the "session key block" is created by using the encrypting session numbers (i.e. the media keys) with the entire set of device keys), but does not specifically teach the encrypted content is generated by encrypting the content using a content key,

on the recording medium, encrypted content key data generated by encrypting the content key using the media keys corresponding to the category of said reproduction apparatus is recorded, and

said reproduction apparatus (a) holds plural device keys, (b) reads out, from the recording medium, the encrypted media key data for the corresponding category, the encrypted content key data for the corresponding category, the encrypted content, and the information regarding the generations of the plural device keys (c) selects one among the plural device keys based on the information regarding the generations of the plural device keys, (d) obtains the media key for the corresponding category by decrypting the encrypted media key data using the selected device key, (e) obtains the content key by decrypting the encrypted content key data using the obtained media key

for the corresponding category, and (f) decrypts the encrypted content using the

obtained content key.

However, Masuda teaches the encrypted content is generated by encrypting the

content using a content key (page 2, lines 49-50, the "scramble key"),

on the recording medium, encrypted content key data generated by encrypting

the content key using the media keys corresponding to the category of said

reproduction apparatus is recorded (page 2, lines 56-58), and

said reproduction apparatus (a) holds plural device keys (Lotspiech, column 1,

line 67 to column 2, line 2), (b) reads out, from the recording medium, the encrypted

media key data for the corresponding category, the encrypted content key data for the

corresponding category, the encrypted content, and the information regarding the

generations of the plural device keys (page 2, line 58 to page 3, line 2) (c) selects one

among the plural device keys based on the information regarding the generations of the

plural device keys (Lotspiech, column 9, lines 14-17), (d) obtains the media key for the

corresponding category by decrypting the encrypted media key data using the selected

device key (Lotspiech, column 2, lines 30-38), (e) obtains the content key by decrypting

the encrypted content key data using the obtained media key for the corresponding

category (page 3, lines 3-5), and (f) decrypts the encrypted content using the obtained

content key (page 3, lines 5-6).

Therefore, it would have been obvious to a person having ordinary skill in the art

at the time the invention was made to modify Lotspiech to encrypt the content using an

additional key as in Masuda because it provides an additional layer of security.

Response to Arguments

14.   Applicant's arguments filed December 29, 2008 have been fully considered but they are not persuasive.

15.   In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., "ease of adding/updating a device key" per page 19 of Applicant's remarks) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

16.   In response to applicant's argument that the references fail to show "a configuration for updating only the device key of a [particular] reproduction terminal … without affecting a [different] reproduction terminal," (page 19 of Applicant's remarks) attention is brought to Lotspiech, column 5, lines 52-54 and column 7, lines 37-56 which clearly established that given unique device keys (which also happens to be a necessary condition of the instant application) a single device (or particular plurality thereof) may be updated or revoked without affecting others.

Conclusion

17.   Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Travis Pogmore whose telephone number is (571)270-

7313. The examiner can normally be reached on Monday through Thursday between

8:30 a.m. and 4:00 p.m. eastern time.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone

number for the organization where this application or proceeding is assigned is 571-

273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/T. P./
Examiner, Art Unit 2436

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2436